

HIGHER DIMENSIONAL FROBENIUS PROBLEM: MAXIMAL SATURATED CONE, GROWTH FUNCTION AND RIGIDITY

AI-HUA FAN, HUI RAO, AND YUAN ZHANG[†]

ABSTRACT. We consider m integral vectors $X_1, \dots, X_m \in \mathbb{Z}^s$ located in a half-space of \mathbb{R}^s ($m \geq s \geq 1$) and study the structure of the additive semi-group $X_1\mathbb{N} + \dots + X_m\mathbb{N}$. We introduce and study maximal saturated cone and directional growth function which describe some aspects of the structure of the semi-group. When the vectors X_1, \dots, X_m are located in a fixed hyperplane, we obtain an explicit formula for the directional growth function and we show that this function completely characterizes the defining data (X_1, \dots, X_m) of the semi-group. The last result will be applied to the study of Lipschitz equivalence of Cantor sets (see [13]).

1. INTRODUCTION

We consider m integral vectors X_1, \dots, X_m in the lattice \mathbb{Z}^s ($m \geq 2, s \geq 1$) which are assumed to be in a half-space. That is to say, there is a vector $\alpha \in \mathbb{R}^s$ such that $\langle X_j, \alpha \rangle > 0$ for all $j = 1, \dots, m$ where $\langle \cdot, \cdot \rangle$ denotes the inner product on the Euclidean space \mathbb{R}^s . We also assume that X_1, \dots, X_m span the vector space \mathbb{R}^s . But X_j 's may not be distinct. Let

$$(1.1) \quad \mathcal{J} = X_1\mathbb{N} + \dots + X_m\mathbb{N}$$

be the semi-group generated by X_1, \dots, X_m where $\mathbb{N} = \{0, 1, 2, \dots\}$ denotes the set of natural numbers. By *higher dimensional Frobenius problem* we mean the study of the structure of the semi-group \mathcal{J} defined by (1.1). This will be our main concern in the present paper.

In the one-dimensional case (i.e. $s = 1$), we are given m relatively prime positive integers a_1, \dots, a_m instead of X_1, \dots, X_m . Then

$$\mathcal{J} = a_1\mathbb{N} + \dots + a_m\mathbb{N}$$

The work is partially supported by NSFC No. 11171128, NSFC No. 11431007, NSFC No.11471132. It is also partially supported by the self-determined research funds of CCNU (No. CCNU14Z01002) from the basic research and operation of MOE. .

Key words and phrases: Frobenius problem, saturated cone, entropy, directional growth function.

[†] The correspondence author.

which is the set of all natural numbers representable as a non-negative integer combination of a_1, \dots, a_m . Sylvester [16] showed that there exists a minimum positive number $f(a_1, \dots, a_m)$, which is now called the Frobenius number, such that

$$f(a_1, \dots, a_m) + 1 + \mathbb{N} \subset \mathcal{J}.$$

The following so-called *diophantine Frobenius Problem* was raised by F. G. Frobenius (see [1]): find $f(a_1, \dots, a_m)$ the largest natural number that is not representable as a non-negative integer combination of a_1, \dots, a_m .

Sylvester's result says that a translation of the set \mathbb{N} is contained in \mathcal{J} . Thus the structure of \mathcal{J} is rather well described by the Frobenius number. It turned out that the knowledge of $f(a_1, \dots, a_m)$ has been extremely useful to investigate many different problems. When $m = 2$, it is well-known that

$$f(a_1, a_2) = a_1 a_2 - a_1 - a_2.$$

For example, if $a_1 = 3$ and $a_2 = 5$, then

$$\mathcal{J} = 3\mathbb{N} + 5\mathbb{N} = \{0, 3, 5, 6, 8, 9, 10, 11, \dots\}$$

and $f(3, 5) = 7$. However, for $m \geq 3$, there is no closed form for $f(a_1, \dots, a_m)$. It is proved that the Frobenius problem is NP-hard under Turing reductions. The book of Ramírez-Alfonsín [1] (2005) is a nice survey on the Frobenius problem.

Our study of higher dimensional Frobenius problem is motivated by the study of Lipschitz equivalence of Cantor sets. Lipschitz equivalence preserves many important properties of a self-similar set. A survey on Lipschitz equivalence of Cantor sets can be found in [12], see also [10]. In this area, a fundamental problem initially raised by Falconer and Marsh [5], which is now called the Falconer-Marsh problem, is as follows: Assume that two self-similar sets E and F are dust-like. How is the Lipschitz equivalence related to the contraction ratios of E and F ? Falconer and Marsh [5] established several basic techniques and results in 1992. But there is no progress until recent works of Rao, Ruan and Wang [11] (2012) and Xiong and Xi [17] (2013).

Xiong and Xi [17] studied the case when E and F have rank 1 (i.e. contraction ratios are powers of a fixed number) and discovered that the problem is closely related to the class number of the field generated by the ratios.

Rao, Ruan and Wang [11] introduce a Lipschitz invariant described by a so-called *matchable condition*. They solved the problem when both E and F have full rank or both of them are two-branch self-similar sets. However, the matchable condition is hard to check

in general. The present paper and the sequential paper [13] introduce new techniques to handle the matchable condition. We associate to each self-similar set a higher dimensional Frobenius problem. We find that this is closely related to the matchable condition. Thanks to this link, in [13], we solve the Falconer-Marsh problem in the case that the contraction ratios of the self-similar sets satisfy a coplanar condition.

In the following subsections we will describe in some detail our results obtained in the paper. Here is a resumé. Two aspects of the structure of the semi-group \mathcal{J} defined by (1.1) will be first studied: one is the existence and finiteness of maximal saturated cones (Section 2) and the other is the growth function which describes how many ways a given vector z in \mathcal{J} can be represented by finite sums of terms from $\{X_1, \dots, X_m\}$. We shall prove that it is a function which increases exponentially as $\|z\|$ tends to the infinity and that the increasing rate depends on the direction along which $\|z\|$ tends to the infinity (Section 3 and Section 4). Thus we obtain the so-called directional growth function. An explicit formula is obtained for the directional growth function when the vectors X_1, \dots, X_m are located on a same hyperplane (Section 5). The last two sections are devoted to the rigidity. The rigidity means, if two growth functions are equal, then the corresponding semi-groups are equal. Furthermore, the sets of vectors defining the semi-groups are the same. These rigidity results are proved under the assumption that the defining vectors are coplanar.

In the following subsections, we state our results in some details.

1.1. Maximal saturated cone. Recall that X_1, \dots, X_m are m given vectors in the lattice \mathbb{Z}^s ($m \geq 2, s \geq 1$) such that $\langle X_j, \alpha \rangle > 0$ for all $j = 1, \dots, m$ and for some vector $\alpha \in \mathbb{R}^s$. For simplicity we use X to denote the set $\{X_1, \dots, X_m\}$. Let

$$(1.2) \quad \mathcal{L} := \mathcal{L}_X := X_1\mathbb{Z} + \dots + X_m\mathbb{Z}$$

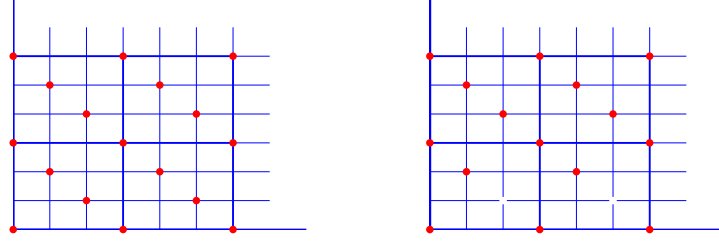
denote the lattice generated by X_1, \dots, X_m . Let

$$(1.3) \quad \mathbf{C}_X := X_1\mathbb{R}^+ + \dots + X_m\mathbb{R}^+$$

denote the convex cone generated by X_1, \dots, X_m , where \mathbb{R}^+ is the set of non-negative real numbers. Clearly, the semi-group \mathcal{J} is a subset of the lattice \mathcal{L} so that

$$\forall g \in \mathcal{J}, \quad (g + \mathbf{C}_X) \cap \mathcal{J} \subset (g + \mathbf{C}_X) \cap \mathcal{L}.$$

If $(g + \mathbf{C}_X) \cap \mathcal{J} = (g + \mathbf{C}_X) \cap \mathcal{L}$, the cone $g + \mathbf{C}_X$ is said to be *saturated*. That means, every lattice point in the cone $g + \mathbf{C}_X$ is in the semi-group. Moreover, a saturated cone is said to be *maximal* if it is not a subset of any other saturated cone. Then we define the

FIGURE 1. Example 1.3: \mathcal{L} (left) and \mathcal{J} (right).

Frobenius set to be

$$(1.4) \quad \mathcal{F} := \{g \in \mathcal{J} : g + \mathbf{C}_X \text{ is a maximal saturated cone}\}.$$

Let us look at the one-dimensional case considered above with $X_j = a_j$. The cone \mathbf{C}_X is then equal to \mathbb{R}^+ . The cone $g + \mathbb{R}^+$ is saturated if and only if $g > f(a_1, \dots, a_m)$. Therefore we have $\mathcal{F} = \{f(a_1, \dots, a_m) + 1\}$, the singleton consisting of the smallest natural number such that all larger natural numbers are representable as a non-negative integer combination of a_1, \dots, a_m .

A natural question is “*how many maximal saturated cones are there ?*” Our answer is

Theorem 1.1. *The Frobenius set \mathcal{F} is non-empty and finite.*

Here is an example where the Frobenius set has two elements. Let $s = 2$ and $X = \{(3, 0), (1, 2), (0, 3)\}$. Then $\mathbf{C}_X = \mathbb{R}^+ \times \mathbb{R}^+$ and

$$\mathcal{L} = \{(a, b) \in \mathbb{Z}^2; a + b \text{ is a multiple of } 3\},$$

$$\mathcal{J} = \{(a, b) \in \mathbb{N}^2; a + b \text{ is a multiple of } 3 \text{ and } b \neq 1\}.$$

We find $\mathcal{F} = \{(1, 2), (0, 3)\}$. This is shown in Figure 1.

1.2. Multiplicity of representations and directional growth function. For any vector z in the semi-group \mathcal{J} , we are interested in the number of representations $z = X_{i_1} + \dots + X_{i_n}$ where $n \geq 1$ and i_k 's are taken from $\{1, 2, \dots, m\}$. As we shall see, these numbers reflect some property of the structure of the semi-group.

Let $\Sigma_m^* := \bigcup_{k=0}^{\infty} \{1, 2, \dots, m\}^k$ be the set of words over the alphabet $\{1, 2, \dots, m\}$, which can also be considered as a tree. For any word $\mathbf{i} = i_1 \dots i_n \in \Sigma_m^*$, define

$$(1.5) \quad \kappa(\mathbf{i}) = X_{i_1} + \dots + X_{i_n}.$$

We consider $\kappa : \Sigma_m^* \rightarrow \mathbb{Z}^s$ as the *walk* in \mathbb{Z}^s guided by X_1, \dots, X_m along with the tree Σ_m^* . Elements in Σ_m^* are also called *pathes* of the walk and $\kappa(\mathbf{i})$ is called the *visited position* following the path \mathbf{i} . A point $z \in \mathbb{Z}^s$ is said to be *attainable* if $z = \kappa(\mathbf{i})$ for some $\mathbf{i} \in \Sigma_m^*$. Clearly the set of attainable positions is exactly the semi-group \mathcal{J} . A second question we ask is “*How many times is an attainable position visited ?*”

To partially answer this question, for $z \in \mathcal{J}$, we define the *multiplicity* of z to be

$$(1.6) \quad \mathbf{m}(z) := \#\{\omega \in \Sigma_m^*; \kappa(\omega) = z\}.$$

We extend the function \mathbf{m} to the convex cone \mathbf{C}_X as follows. For any point $x \in \mathbf{C}_X$ but not in \mathcal{J} , instead of setting $\mathbf{m}(x) = 0$, we define its multiplicity to be the multiplicity of the point in \mathcal{J} which is nearest to x . More precisely,

$$(1.7) \quad \mathbf{m}(x) := \min\{\mathbf{m}(z); z \in \mathcal{J} \text{ and } \|x - z\| = d(x, \mathcal{J})\},$$

where $\|\cdot\|$ denotes the Euclidean norm and $d(x, \mathcal{J}) := \min\{\|x - z\|; z \in \mathcal{J}\}$.

In the one-dimensional case, the multiplicity \mathbf{m} restricted on \mathcal{J} satisfies the linear recurrent relation

$$\mathbf{m}(n) = \sum_{j=1}^m \mathbf{m}(n - a_j).$$

Hence we can obtain an explicit formula for $\mathbf{m}(n)$. It is then easy to show that $\mathbf{m}(n)$ is of the same exponential order as β^n where β is the largest root of the equation

$$x^{a_m} - \sum_{j=1}^m x^{a_m - a_j} = 0.$$

(See, for instance, [2]). But in the higher dimensional case, it is hard to obtain an explicit formula for the multiplicity. Nevertheless, we will prove the following exponential growth.

Theorem 1.2. *For any unit vector $\theta \in \mathbf{C}_X$, the following limit exists*

$$(1.8) \quad \gamma(\theta) = \lim_{k \rightarrow \infty} \frac{\log \mathbf{m}(k\theta)}{k}.$$

We call γ the *directional growth function* of the semi-group \mathcal{J} . It describes the exponential increasing speed of the multiplicity along the direction θ . We will first prove that the multiplicity function varies slowly in the sense that the quotient of $\mathbf{m}(z)$ and $\mathbf{m}(z')$ is of polynomial order of $\|z\|$ if z' and z have a bounded distance (Theorem 3.3). We will then prove that the sequence $(\log \mathbf{m}(k\theta))_{k \geq 1}$ is subadditive in some weak sense, which is sufficient to ensure the existence of the limit in (1.8), according to Lemma 4.1 which strengthens a classical result on sub-additive sequence.

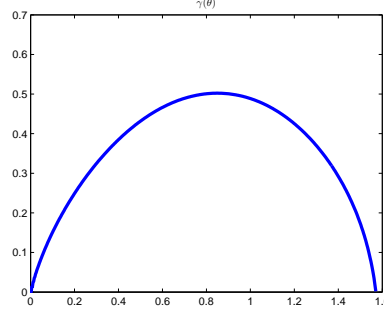


FIGURE 2. The function $\gamma(\theta)$ for $X = \{(3, 0), (1, 2), (0, 3)\}$.

1.3. Calculation of $\gamma(\theta)$ when X_1, \dots, X_m are coplanar. In general, it is difficult to obtain an explicit formula of $\gamma(\theta)$. We will be confined to a formula under the condition that X_1, \dots, X_m are coplanar.

We say that X_1, \dots, X_m are *coplanar* if they locate on a same hyper-plane, i.e. there exists a vector $\eta \in \mathbb{R}^s$ such that

$$(1.9) \quad \langle \eta, X_j \rangle = 1, \quad j = 1, \dots, m.$$

To be more precise, we say X_1, \dots, X_m are η -coplanar. Let $p = (p_1, \dots, p_m)$ be a probability vector. The *entropy* of p is defined as

$$h(p) = - \sum_{j=1}^m p_j \log p_j.$$

Theorem 1.3. *Suppose that X_1, \dots, X_m are η -coplanar. For any unit vector θ in the cone \mathbf{C}_X , we have*

$$(1.10) \quad \gamma(\theta) = \langle \theta, \eta \rangle \sup \left\{ h(p); p_1 X_1 + \dots + p_m X_m = \frac{\theta}{\langle \theta, \eta \rangle} \right\}.$$

There is another expression involving the following function $\log \sum_{j=1}^m e^{\langle t, X_j \rangle}$, $t \in \mathbb{R}^s$, which corresponds to the pressure function in the statistic physics (Theorem 6.2). The above formula (1.10) resembles the conditional variation principle in the analysis of multifractal analysis (see [7], see also [6], [8]). Actually, the proof of Theorem 1.3 uses the idea of large deviation. If X_1, \dots, X_m are linearly independent, then the choice of p is unique and we can easily compute $\gamma(\theta)$.

Here is an example. Let $s = 2$ and $X = \{(1, 0), (0, 1)\}$. Then $\mathbf{C}_X = (\mathbb{R}^+)^2$, $\mathcal{J} = \mathbb{N}^2$, $\mathcal{L} = \mathbb{Z}^2$ and $\eta = (1, 1)$. Clearly $\mathbf{m}(a, b) = \frac{(a+b)!}{a!b!}$. For $\theta = (\theta_1, \theta_2)$ with $\theta_1^2 + \theta_2^2 = 1$ and $\theta_1, \theta_2 \geq 0$. Let $p_1 = \theta_1/(\theta_1 + \theta_2)$, $p_2 = \theta_2/(\theta_1 + \theta_2)$. This vector (p_1, p_2) is the unique

probability satisfying $p_1X_1 + p_2X_2 = \theta/\langle\eta, \theta\rangle$. Then

$$\gamma(\theta) = (\theta_1 + \theta_2)h(p_1, p_2).$$

The unit vector (θ_1, θ_2) can be described by the angle $\alpha \in [0, \pi/2]$ such that $\theta_1 = \cos \alpha$. Then

$$\gamma(\alpha) = -\cos \alpha \log \frac{\cos \alpha}{\cos \alpha + \sin \alpha} - \sin \alpha \log \frac{\sin \alpha}{\cos \alpha + \sin \alpha}.$$

The maximum is attained at $\pi/4$ and $\gamma(\pi/4) = \sqrt{2} \log 2$. The formula of $\gamma(\theta)$ in this case can be directly deduced from the Stirling formula.

Here is another example where $X = \{(3, 0), (1, 2), (0, 3)\}$. The graph of the growth function $\gamma(\theta)$ is shown in Figure 2.

1.4. Rigidity results. Given two sets of vectors $X = \{X_1, \dots, X_m\}$ and $Y = \{Y_1, \dots, Y_{m'}\}$ in \mathbb{Z}^s . Suppose that they define the same directional growth function, *i.e.*

$$(1.11) \quad \mathbf{C}_X = \mathbf{C}_Y \text{ and } \gamma_X = \gamma_Y.$$

What can we say about X and Y ? In our terminology, Rao, Ruan and Wang [11] proved the following rigidity result.

Proposition 1.4 ([11]). *Suppose $X = \{X_1, \dots, X_s\}$ and $Y = \{Y_1, \dots, Y_s\}$ are two sets of linearly independent vectors in \mathbb{Z}^s . If they define the same directional growth function, then X is a permutation of Y .*

We will generalize the above result to the coplanar case. Notice that X_1, \dots, X_m are coplanar if $m \leq s$ and in particular, linearly independent vectors are coplanar.

Theorem 1.5. *Suppose $X = \{X_1, \dots, X_m\}$ and $Y = \{Y_1, \dots, Y_{m'}\}$ are η -coplanar for some $\eta \in \mathbb{R}^s$ and that they define the same directional growth function. Then $m = m'$ and X is a permutation of Y .*

As we shall see, the proof Theorem 1.5 is much more difficult than that of Proposition 1.4. We can still consider two coplanar sets of vectors which are respectively located on two different hyper-planes.

Let $X^{(p)} = (\kappa(\mathbf{i}))_{\mathbf{i} \in \{1, \dots, m\}^p}$, which is called the p -th iteration of X , where κ is defined in (1.5). For example, the second iteration of $X = \{(1, 0), (0, 1)\}$ is $\{(2, 0), (1, 1), (1, 1), (0, 2)\}$. Using techniques of algebraic plane curve, we prove that

Theorem 1.6. *Suppose $X = \{X_1, \dots, X_m\}$ is η -coplanar and $Y = \{Y_1, \dots, Y_{m'}\}$ is η' -coplanar, and suppose X and Y define the same directional growth function. Then $\eta = c\eta'$*

for some $c > 0$ and there exists two integers $n, n' \geq 1$ such that the n -th iteration of X is a permutation of the n' -th iteration of Y .

1.5. Relation to the Lipschitz equivalence of Cantor sets. Let $\boldsymbol{\rho} = (\rho_1, \dots, \rho_m)$ be a vector such that $\rho_j \in (0, 1)$ for all $j = 1, 2, \dots, m$. An example is the set of contraction ratios in a contractive self-similar iterated function system. Let $\langle \boldsymbol{\rho} \rangle$ (resp. $\langle \boldsymbol{\rho} \rangle_+$) denote the subgroup (resp. semi-group) of (\mathbb{R}^+, \times) generated by ρ_1, \dots, ρ_m . Such semi-groups $\langle \boldsymbol{\rho} \rangle_+$ play a crucial role in the discussion of the Lipschitz equivalence of self-similar Cantor sets ([5]).

A *pseudo-basis* of $\langle \boldsymbol{\rho} \rangle$ is a set of numbers $\boldsymbol{\lambda} = (\lambda_1, \dots, \lambda_s)$ such that $\langle \boldsymbol{\rho} \rangle \subset \langle \boldsymbol{\lambda} \rangle$ and s is the rank of $\langle \boldsymbol{\rho} \rangle$, i.e. the cardinality of a basis of $\langle \boldsymbol{\rho} \rangle$. The multiplicative group $\langle \boldsymbol{\lambda} \rangle$ is isomorphic to the additive group $(\mathbb{Z}^s, +)$ and an isomorphism is defined by $\exp_{\boldsymbol{\lambda}} : \mathbb{Z}^s \rightarrow \langle \boldsymbol{\lambda} \rangle$ where

$$\forall X = (X^1, \dots, X^s) \in \mathbb{Z}^s, \quad X \mapsto \boldsymbol{\lambda}^X := \prod_{i=1}^s \lambda_i^{X^i}.$$

The inverse map $\log_{\boldsymbol{\lambda}} : \langle \boldsymbol{\lambda} \rangle \rightarrow \mathbb{Z}^s$ of the isomorphism is then defined by $\log_{\boldsymbol{\lambda}} x = X$ for $x = \boldsymbol{\lambda}^X \in \langle \boldsymbol{\lambda} \rangle$. Let

$$X_i = \log_{\boldsymbol{\lambda}} \rho_i, \quad (i = 1, \dots, m).$$

Then the multiplicative semi-group $\langle \boldsymbol{\rho} \rangle_+$ is isomorphic to the additive semi-group $\mathcal{J}(\boldsymbol{\rho}) = X_1\mathbb{N} + \dots + X_m\mathbb{N}$.

Given two Cantor sets generated by self-similar iterated function systems. We fix a common pseudo-basis $\boldsymbol{\lambda}$ for both sets of contractions, denoted $\boldsymbol{\rho}$ and $\boldsymbol{\rho}'$. Such a pseudo-basis does exist when the two Cantor sets are Lipschitz equivalent ([5]). Under the assumption that both sets of vectors $\log_{\boldsymbol{\lambda}} \boldsymbol{\rho}$ and $\log_{\boldsymbol{\lambda}} \boldsymbol{\rho}'$ are coplanar, it will be proved that two such Cantor sets are Lipschitz equivalent if and only if the situation described in the rigidity Theorem 1.6 takes place (see [13]).

2. Maximal saturated cones

We assume that $X_1, \dots, X_m \in \mathbb{Z}^s$ locate on a same half-plane, that is, there exists a vector $\boldsymbol{\alpha} \in \mathbb{R}^s$ such that $\langle X_j, \boldsymbol{\alpha} \rangle > 0$ for $j = 1, \dots, m$. Recall that $\mathbf{C}_X = X_1\mathbb{R}^+ \dots + X_m\mathbb{R}^+$ and $\mathcal{L} = X_1\mathbb{Z} + \dots + X_m\mathbb{Z}$ are respectively the cone and the lattice generated by X_1, \dots, X_m .

Remark that we can work in a little more general setting. Let E be a Euclidean space and L be a lattice of full rank in E . Given m non-zero points X_1, \dots, X_m of the lattice, we can consider the generated semi-group $\mathbb{N}X_1 + \dots + \mathbb{N}X_m$. In other word, there is no need

to work with the orthogonal lattice \mathbb{Z}^d . All the results we will present remain true in this setting.

Theorem 2.1. *There exists $g \in \mathcal{J}$ such that $g + \mathbf{C}_X$ is a saturated cone.*

Proof. Set $\Omega = \left\{ \sum_{j=1}^m c_j X_j; c_j \in [0, 1] \right\}$, considered as basic domain. Then every $x = c_1 X_1 + \cdots + c_m X_m \in \mathbf{C}_X$ can be written as

$$(2.1) \quad x = y + \omega$$

where $y = \lfloor c_1 \rfloor X_1 + \cdots + \lfloor c_m \rfloor X_m$ is in the semi-group \mathcal{J} and $\omega \in \Omega$. Let

$$\Omega^* = \Omega \cap \mathcal{L}.$$

Since Ω is bounded, Ω^* is a finite set. Then there exists an integer M such that for every $\omega \in \Omega^*$, there exists $a_1, \dots, a_m \in \mathbb{Z}$ such that

$$\omega = \sum_{j=1}^m a_j X_j, \quad |a_j| \leq M.$$

Put $g = M(X_1 + \cdots + X_m)$. We claim that the cone $g + \mathbf{C}_X$ is saturated.

In fact, let $z \in (g + \mathbf{C}_X) \cap \mathcal{L}$. Since $z - g \in \mathbf{C}_X$, as we have just seen, we can write

$$z - g = x + \omega, \quad \text{with } x \in \mathcal{J}, \omega \in \Omega.$$

Since z , g and x all belong to \mathcal{L} , so does ω . Hence $\omega \in \Omega^*$. By the definition of g , it is clear that $g + \omega \in \mathcal{J}$. Thus $z = x + (g + \omega) \in \mathcal{J}$. \square

Proof of Theorem 1.1. The existence of saturated cones is confirmed by Theorem 2.1. For a given saturated cone, there is at most a finite number of saturated cones which contain the given one. This finiteness implies the existence of maximum saturated cone.

In the following, we show that the number of maximal saturated cones is finite by contradiction. Suppose on the contrary that the Frobenius set \mathcal{F} is infinite. For any $g \in \mathcal{F}$, choose a path ω such that $g = \kappa(\omega)$ and set $u(g) = (u_1, \dots, u_m)$ where u_j counts the number of the symbol j in ω . (We remark that the choice of ω is not unique.)

By the definition of maximal saturated cone, for any $g_1, g_2 \in \mathcal{F}$, both $g_1 - g_2$ and $g_2 - g_1$ do not belong to \mathcal{J} . Hence, $u(g_1)$ and $u(g_2)$ are not comparable, *i.e.*, both $u(g_1) - u(g_2)$ and $u(g_2) - u(g_1)$ are not non-negative vectors. However, since the set $\{u(g); g \in \mathcal{F}\} \subset \mathbb{N}^m$ is infinite, there must exist two comparable elements. This contradiction proves the theorem. \square

As a direct consequence of (2.1), we have

Lemma 2.2. *The set \mathcal{J} is relatively dense in \mathbf{C}_X , that is, there exists a constant $R_0 > 0$ such that $d(x, \mathcal{J}) < R_0$ for every $x \in \mathbf{C}_X$.*

3. Variation of multiplicity function

We are now going to prove that the multiplicity $\mathbf{m}(z)$ has an exponential increasing rate as z tends to the infinity along each direction in the cone \mathbf{C}_X .

First of all, we give another expression for the multiplicity function \mathbf{m} . For $z \in \mathcal{J}$, define

$$(3.1) \quad A(z) := \left\{ (u_1, \dots, u_m) \in \mathbb{N}^m; \sum_{j=1}^m u_j X_j = z \right\}.$$

The cardinality $\#A(z)$ is the number of ways that z can be represented as linear combination of X_1, \dots, X_m with non-negative integer coefficients. In one dimensional case, the function $z \mapsto \#A(z)$ is the *denumerant function* introduced by Sylvester [16]. We have the following expression for $\mathbf{m}(z)$:

$$(3.2) \quad \mathbf{m}(z) = \sum_{u \in A(z)} \frac{|u|!}{u!}$$

where $|u| = u_1 + \dots + u_m$ and $u! = u_1! \dots u_m!$ for a multi-index $u = (u_1, \dots, u_m) \in \mathbb{N}^m$.

Assume $X = \{(1, 0), (0, 1)\}$. Then $\mathcal{J} = \mathbb{N}^2$ and for $(a, b) \in \mathbb{N}^2$, we have

$$\mathbf{m}(a, b) = \frac{(a+b)!}{a!b!}.$$

Hence if the distance of two points (a, b) and (a', b') are bounded by a constant, we see that $\mathbf{m}(a, b)/\mathbf{m}(a', b')$ is controlled by a polynomial of $\sqrt{a^2 + b^2}$. As we shall show in Theorem 3.3, that is the case in general.

For $z = (z^1, \dots, z^s) \in \mathbb{R}^s$, define $\|z\|_\infty := \max\{|z^1|, \dots, |z^s|\}$. Let d_H denote the Hausdorff metric, that is, if A and B are two subsets of \mathbb{R}^s , then

$$d_H(A, B) = \max \left\{ \sup_{a \in A} d(a, B), \sup_{b \in B} d(b, A) \right\}.$$

Recall that $\langle X_j, \alpha \rangle > 0$ for all $j \in \{1, \dots, m\}$. Set

$$(3.3) \quad \delta = \min_{1 \leq j \leq m} \frac{\langle X_j, \alpha \rangle}{\|\alpha\|}.$$

Lemma 3.1. *The set $A(z)$ is contained in a $\|\cdot\|_\infty$ -ball of radius $\|z\|/\delta$. In other word, $\|u\|_\infty \leq \|z\|/\delta$ for all $u \in A(z)$.*

Proof. Let $u \in A(z)$ so that $z = \sum_{j=1}^m u_j X_j$. Using Schwartz inequality, we obtain

$$\|z\| \geq \frac{\langle z, \alpha \rangle}{\|\alpha\|} = \sum_{j=1}^m u_j \frac{\langle X_j, \alpha \rangle}{\|\alpha\|} \geq \delta \|u\|_\infty.$$

The lemma follows. \square

The following theorem plays a crucial rôle in our argument.

Theorem 3.2. *Let $C_0 \geq 1$ be an integer. Then there exists an integer $M > 0$ such that*

$$d_H(A(z), A(z')) < M,$$

provided that $z, z' \in \mathcal{J}$ and $\|z - z'\| \leq C_0$.

Proof. For $u, v \in \mathbb{R}^m$, we define the order $u \preceq v$ if $v - u$ is a non-negative vector. Pick any $u = (u_1, \dots, u_m) \in A(z)$. We claim that there exists $z^* \in \mathcal{J}$ such that

- (i) there exists $u^* \in A(z^*)$ such that $u^* \preceq u$ (this implies that $z - z^* \in \mathcal{J}$);
- (ii) $z' - z^* \in \mathcal{J}$;
- (iii) $\|z - z^*\| \leq M'$, where M' is a constant depending only on X_1, \dots, X_m and C_0 .

Notice that $z = z^* + (z - z^*)$ and $z' = z^* + (z' - z^*)$ with $z^*, z - z^*, z' - z^*$ belonging to \mathcal{J} . Roughly speaking, the point z^* is not far away from z and one can walk from 0 to z^* . From there one can walk to z as well as to z' . (See Figure 3 left.)



FIGURE 3.

Suppose the claim is proved. Take any $v' = (v'_1, \dots, v'_m) \in A(z' - z^*)$ and set $v = u^* + v'$. Then $v \in A(z')$ and

$$\begin{aligned} \|u - v\|_\infty &\leq \|u - u^*\|_\infty + \|v - u^*\|_\infty \\ &\leq (\|z - z^*\| + \|z' - z^*\|)/\delta \quad (\text{By Lemma 3.1}) \\ &\leq (2M' + C_0)/\delta. \end{aligned}$$

We have thus proved the theorem by choosing $M = \sqrt{m}(2M' + C_0)/\delta$.

Now it suffices to prove the claim. Take $x_0 \in \mathcal{J}$ such that $B(x_0, C_0) \subset \mathbf{C}_X$, where $B(x, r)$ denotes the ball with center x and radius r . Take $g \in \mathcal{J}$ such that $g + \mathbf{C}_X$ is a

saturated cone. We will prove the claim by distinguishing two cases according to whether $z \in g + x_0 + \mathbf{C}_X$.

Case 1: $z \in g + x_0 + \mathbf{C}_X$.

A point $\tilde{z} = \sum_{j=1}^m \tilde{u}_j X_j$ is called a *first entering position* if $\tilde{u} = (\tilde{u}_1, \dots, \tilde{u}_m)$ is a minimal vector (w.r.t. the order \preceq) such that $\tilde{z} \in g + x_0 + \mathbf{C}_X$ and $\tilde{u} \preceq u$. Such \tilde{z} do exist, but may not be unique (See Figure 3 right). We fix such a point \tilde{z} and set $z^* = z - \tilde{z}$. Since $\tilde{u} \preceq u$, we have $z^* \in \mathcal{J}$. We are going to check that (i)-(iii) hold for this z^* .

(i) holds since $\tilde{u} \preceq u$.

From $z - z^* = \tilde{z} \in g + x_0 + \mathbf{C}_X$ we deduce that $z - z^* - x_0 \in g + \mathbf{C}_X$. This, together with $\|z - z'\| \leq C_0$, implies

$$z' - z^* \in B(z, C_0) - z^* = z - z^* - x_0 + B(x_0, C_0) \subset (z - z^* - x_0) + \mathbf{C}_X \subset g + \mathbf{C}_X.$$

Hence $z' - z^* \in (g + \mathbf{C}_X) \cap \mathcal{L}$, and so that $z' - z^* \in \mathcal{J}$ by the saturation property of $g + \mathbf{C}_X$. This proves the property (ii).

Recall that $\tilde{z} \in g + x_0 + \mathbf{C}_X$. The minimality of \tilde{z} implies

$$\tilde{z} \in (g + x_0) + \left\{ \sum_{j=1}^m c_j X_j; 0 \leq c_j < 1 \right\}.$$

It follows that

$$\|z - z^*\| = \|\tilde{z}\| \leq \|g + x_0\| + \sum_{j=1}^m \|X_j\| := M',$$

and hence (iii) holds.

Case 2. $z \notin g + x_0 + \mathbf{C}_X$.

In this case, we could say that z is close to a face of the cone \mathbf{C}_X . Indeed, the boundary of \mathbf{C}_X can be written as

$$\partial \mathbf{C}_X = \bigcup_{j=1}^N \mathcal{D}_j,$$

where \mathcal{D}_j are faces of \mathbf{C}_X , which are cones of dimension $s - 1$. Let \vec{n}_j be the unit vector perpendicular to \mathcal{D}_j and pointing to the half-space containing \mathbf{C}_X , that is to say, $\langle \vec{n}_j, x \rangle \geq 0$ for all $x \in \mathbf{C}_X$. We note that $x \in \mathbf{C}_X$ if and only if $\langle \vec{n}_j, x \rangle \geq 0$ for all $j \in \{1, \dots, N\}$.

Since $z \notin g + x_0 + \mathbf{C}_X$, there exists an integer $j_0 \in \{1, \dots, N\}$ such that $\langle \vec{n}_{j_0}, z - (g + x_0) \rangle < 0$, namely,

$$(3.4) \quad \langle z, \vec{n}_{j_0} \rangle < \langle g + x_0, \vec{n}_{j_0} \rangle,$$

which means that z is closer to the face \mathcal{D}_{j_0} than $g + x_0$. Let $\Omega_{j_0} = \{i; \langle X_i, \vec{n}_{j_0} \rangle = 0\}$. Take any $u = (u_1, \dots, u_m) \in A(z)$ and set

$$z_1 = \sum_{i \in \Omega_{j_0}} u_i X_i.$$

Clearly, $z_1 \in \mathcal{D}_{j_0}$. Denote $\delta' = \min\{\langle X_i, \vec{n}_{j_0} \rangle; i \in \{1, \dots, m\} \setminus \Omega_{j_0}\}$. Since $\langle X_j, \vec{n}_{j_0} \rangle \geq 0$ for all $j \in \{1, 2, \dots, m\}$, we deduce that for all $i \in \{1, \dots, m\} \setminus \Omega_{j_0}$ we have

$$u_i \leq \frac{\langle z, \vec{n}_{j_0} \rangle}{\delta'} \leq \frac{\langle g + x_0, \vec{n}_{j_0} \rangle}{\delta'} := M_1.$$

It follows that

$$(3.5) \quad \|z - z_1\| \leq mM_1 \max_{1 \leq j \leq m} \|X_j\|.$$

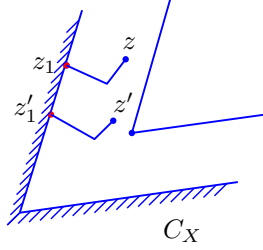


FIGURE 4.

Take any $v = (v_1, \dots, v_m) \in A(z')$ and set $z'_1 = \sum_{i \in \Omega_{j_0}} v_i X_i$. Then $z'_1 \in \mathcal{D}_{j_0}$. A similar argument as above shows that $v_i \leq M_1 + C_0/\delta' := M_2$, for all $i \in \{1, \dots, m\} \setminus \Omega_{j_0}$, and

$$(3.6) \quad \|z' - z'_1\| \leq mM_2 \max_{1 \leq j \leq m} \|X_j\|.$$

According to (3.5) and (3.6), to prove the claim holds for z and z' , we only need prove that the claim hold for z_1 and z'_1 . That is say, suppose we can walk from the origin to a suitable point z_1^* and then walk from z_1^* to z_1 as well as to z'_1 . These walks remains in the lower dimensional cone \mathcal{D}_{j_0} . Of cause, we can finally walk to z and to z' . Observe that

$$\|z_1 - z'_1\| < m(M_1 + M_2) \max_{1 \leq j \leq m} \|X_j\| + C_0.$$

The claim can thus be proved by induction on the dimension of the cone. \square

The following theorem asserts that $\mathbf{m}(z)$ varies not so rapidly. Theorem 3.2 will be useful for its proof.

Theorem 3.3. *Let $C_0 \geq 1$ be an integer. There exists a polynomial $Q(x)$ with positive coefficients such that*

$$\frac{1}{Q(\|z\|)} \leq \frac{\mathbf{m}(z)}{\mathbf{m}(z')} \leq Q(\|z\|)$$

provided that $z, z' \in \mathcal{J}$ and $\|z - z'\| \leq C_0$.

Proof. Let M be the constant in Theorem 3.2, which depends on C_0 . There exists a polynomial $G(x)$ (depending on m and M) with positive coefficients such that

$$\frac{|v|!}{|u|!} \cdot \frac{u!}{v!} \leq G(\|u\|)$$

holds for all $u, v \in \mathbb{N}^m$ such that $\|u - v\| \leq M$. In other word,

$$\frac{|u|!}{u!} \geq \frac{1}{G(\|u\|)} \frac{|v|!}{v!}.$$

We can take $G(x) = x^{2mM}$. Denoting by N_0 the number of integer points in the ball $B(0, M)$, we have

$$(3.7) \quad N_0 \frac{|u|!}{u!} \geq \frac{1}{G(\|u\|)} \sum_{v: \|u-v\| \leq M} \frac{|v|!}{v!}.$$

Summing up both sides of (3.7) over $u \in A(z)$, we obtain

$$(3.8) \quad N_0 \sum_{u \in A(z)} \frac{|u|!}{u!} \geq \frac{1}{G(\|u^*\|)} \sum_{u \in A(z)} \left(\sum_{v: \|u-v\| \leq M} \frac{|v|!}{v!} \right) \geq \frac{1}{G(\|u^*\|)} \sum_{v \in A(z')} \frac{|v|!}{v!},$$

where u^* is a point in $A(z)$ such that $\|u^*\|$ attains the maximum. The last inequality holds because

$$A(z') \subset \bigcup_{u \in A(z)} \{v \in \mathbb{N}^s; \|u - v\| \leq M\}$$

by Theorem 3.2. By recalling the expression (3.2) for $\mathbf{m}(z)$, we see that (3.8) is nothing but

$$\frac{\mathbf{m}(z)}{\mathbf{m}(z')} \geq \frac{1}{N_0 G(\|u^*\|)}.$$

Since $\|u^*\| \leq m\|u^*\|_\infty \leq m\|z\|/\delta$ (by Lemma 3.1), where δ is defined by (3.3), we have

$$\frac{1}{N_0 G(m\|z\|/\delta)} \leq \frac{\mathbf{m}(z)}{\mathbf{m}(z')} \leq N_0 G(m\|z'\|/\delta)$$

where the second inequality is obtained from the first one by symmetry. Notice that $\|z'\| \leq \|z\| + C_0$. We have thus proved the theorem with $Q(x) = N_0 G(\delta^{-1}m(x + C_0))$. \square

4. Existence of directional growth

In this section we prove the existence of the limit defining the directional growth $\gamma(\theta)$. Recall that the multiplicity of a point in \mathbf{C}_X is defined as

$$\mathbf{m}(x) = \min\{\mathbf{m}(z) : z \in \mathcal{J} \text{ and } \|x - z\| = d(x, \mathcal{J})\}.$$

Proof of Theorem 1.2. Fix a unit vector θ in \mathbf{C}_X . Let us denote z_k to be the point in \mathcal{J} such that

$$\mathbf{m}(k\theta) = \mathbf{m}(z_k), \quad d(k\theta, z_k) = d(k\theta, \mathcal{J}).$$

By the relative density of \mathcal{J} (Lemma 2.2), there exists a constant $R_0 > 0$ such that

$$(4.1) \quad \|z_k - k\theta\| < R_0$$

for all k and all θ . By the definition of multiplicity, it is obvious that $\mathbf{m}(z+z') \geq \mathbf{m}(z)\mathbf{m}(z')$ for any $z, z' \in \mathcal{J}$. In particular, for any $n, p \geq 1$,

$$(4.2) \quad \mathbf{m}(z_n + z_p) \geq \mathbf{m}(z_n)\mathbf{m}(z_p).$$

As consequence of (4.1), we have $\|z_{n+p} - (z_n + z_p)\| \leq 3R_0$. Hence, by Theorem 3.3, there exists a polynomials $Q(x)$ with positive coefficients such that

$$\mathbf{m}(z_{n+p}) \geq \frac{1}{Q(\|z_{n+p}\|)} \mathbf{m}(z_n + z_p) \geq \frac{1}{Q(\|z_{n+p}\|)} \mathbf{m}(z_n)\mathbf{m}(z_p).$$

Using the fact $\mathbf{m}(k\theta) = \mathbf{m}(z_k)$ for all k , we get then

$$\mathbf{m}((n+p)\theta) \geq \frac{1}{\tilde{Q}(n+p)} \mathbf{m}(n\theta)\mathbf{m}(p\theta),$$

where $\tilde{Q}(x) = Q(x + R_0)$. Here we used the observation that $\|z_{n+p}\| \leq (n+p) + R_0$ and the fact that $Q(x)$ has positive coefficients to get $Q(\|z_{n+p}\|) \leq \tilde{Q}(n+p)$. Observe that $\log \tilde{Q}(n+p) \leq c \log(n+p)$ for some constant $c > 0$. We can finish the proof by using the next lemma to $b_n = \log \mathbf{m}(n\theta)$. \square

It is well known that if a sequence b_n is sub-additive, *i.e.*, $b_n + b_m \leq b_{n+m}$, then the limit $\lim b_n/n$ exists. The following lemma strengthen this result.

Lemma 4.1. *Let $c > 0$ be a constant. If $\{b_n\}$ be a sequence in \mathbb{R}^+ such that*

$$(4.3) \quad b_n + b_m \leq b_{n+m} + c \log(m+n), \quad \text{for all } m, n \geq 1,$$

then the limit $\lim_{n \rightarrow \infty} b_n/n$ exists.

Proof. Without loss of generality, we can assume $c = 1$, otherwise we consider $c^{-1}b_n$ instead of b_n . Fix a positive integer m . By (4.3) we have

$$(4.4) \quad \forall s \geq 1, \quad b_{2^s m} \geq 2b_{2^{s-1}m} - \log(2^s m).$$

Fix a positive integer $l \geq 1$. For $1 \leq s \leq l$, as consequence of (4.4) we get

$$(4.5) \quad b_{2^l m} \geq 2^l b_m - [2^{l-1} \log(2m) + 2^{l-2} \log(4m) + \cdots + \log(2^l m)] = 2^l b_m - g(m, l)$$

where

$$g(m, l) = (2^{l+1} - 2 - l) \log 2 + (2^l - 1) \log m.$$

For any $n \in \mathbb{N}$, we write $n = Lm + r$ with $0 \leq r < m$. By (4.3), we have

$$b_n \geq b_{Lm} + b_r - \log n.$$

In order to estimate b_{Lm} , we use L 's dyadic expansion $L = 2^{l_1} + 2^{l_2} + \cdots + 2^{l_k}$ where $l_1 > l_2 > \cdots > l_k \geq 0$. Obviously $\log_2 L - 1 \leq l_1 \leq \log_2 L$. Using (4.3) then (4.5), we obtain

$$\begin{aligned} b_{Lm} &\geq b_{2^{l_1}m} + b_{(2^{l_2} + \cdots + 2^{l_k})m} - \log((2^{l_1} + 2^{l_2} + \cdots + 2^{l_k})m) \\ &\geq 2^{l_1} b_m - g(m, l_1) - \log((2^{l_1} + 2^{l_2} + \cdots + 2^{l_k})m) + b_{(2^{l_2} + \cdots + 2^{l_k})m}. \end{aligned}$$

Hence, by induction, we have

$$b_{Lm} \geq \sum_{j=1}^{k-1} \left(2^{l_j} b_m - g(m, l_j) - \log((2^{l_j} + \cdots + 2^{l_k})m) \right) + 2^{l_k} b_m - g(m, l_k).$$

Note that $\sum_{j=1}^k 2^{l_j} = L$ and

$$\begin{aligned} \sum_{j=1}^k g(m, l_j) &\leq \sum_{j=1}^k 2^{l_j} \log 4m \leq L \log(4m), \\ \sum_{j=1}^{k-1} \log((2^{l_j} + \cdots + 2^{l_k})m) &\leq l_1 \log(Lm) \leq \log_2 n \log n. \end{aligned}$$

Hence we have

$$b_{Lm} \geq Lb_m - L \log 4m - \log_2 n \log n.$$

Dividing both sides by n , taking the liminf and using the fact $L/n \rightarrow m$, we have

$$(4.6) \quad \liminf_{n \rightarrow \infty} \frac{b_n}{n} \geq \frac{b_m - \log 4m}{m}.$$

Then taking the limsup as $m \rightarrow \infty$ finishes the proof. \square

5. Principle of Maximal entropy under linear constraints

Let Δ_m be the simplex of all probability measures $p = (p_1, \dots, p_m)$. The entropy function $h(p)$ is defined on Δ_m as follows

$$h(p) = - \sum_{j=1}^m p_j \log p_j.$$

Let X_1, \dots, X_m be m given vectors in a Euclidean space \mathbb{R}^d . We will consider the maximum of $h(p)$ under the constraints

$$(5.1) \quad \sum_{j=1}^m p_j = 1, \quad \sum_{j=1}^m p_j X_j = \beta$$

for any β in the convex hull generated by $X = \{X_1, \dots, X_m\}$ which is defined by

$$\Delta_X = \left\{ \sum_{j=1}^m p_j X_j : (p_1, \dots, p_m) \in \Delta_m \right\}.$$

When $d = 1$, the solution is given by the principle of maximum entropy due to Jaynes [9].

Let us define

$$Z(t) = \sum_{j=1}^m e^{\langle t, X_j \rangle}, \quad t \in \mathbb{R}^d.$$

We have

$$\nabla Z(t) = \sum_{j=1}^m X_j e^{\langle t, X_j \rangle}$$

Theorem 5.1. *Suppose that the vectors X_1, \dots, X_m are not coplanar and β is in the interior of Δ_X . Then under the constraints $\sum_{j=1}^m p_j = 1$ and $\sum_{j=1}^m p_j X_j = \beta$, the entropy function $h(p)$ attains its maximum at the maximal point p^* defined by*

$$(5.2) \quad p_j^* = \frac{e^{\langle t_\beta, X_j \rangle}}{Z(t_\beta)} \quad (j = 1, 2, \dots, m)$$

where t_β is the unique solution of the equation

$$(5.3) \quad \frac{\nabla Z(t)}{Z(t)} = \beta.$$

Actually the maximal point is unique and the maximum entropy is equal to

$$h(p^*) = \log Z(t_\beta) - \langle t_\beta, \beta \rangle.$$

The map $\beta \mapsto t_\beta$ is C^∞ -diffeomorphism from $\overset{\circ}{\Delta}_X$ onto \mathbb{R}^d .

The proof of the theorem will be decomposed into several lemmas.

We will denote by $\overset{\circ}{A}$ the interior of a set A . Let $M : \mathbb{R}^m \rightarrow \mathbb{R}^d$ the linear map defined by the $d \times m$ matrix

$$M = (X_1, \dots, X_m).$$

Lemma 5.2. $\overset{\circ}{\Delta}_X = M(\overset{\circ}{\Delta}_m)$.

Proof. Notice that $Mp = \sum_{j=1}^m p_j X_j$. Let $\pi : \mathbb{R}^m \rightarrow \mathbb{R}^m / \ker(M)$ be the canonical map from \mathbb{R}^m to the quotient space $\mathbb{R}^m / \ker(M)$ and let \widetilde{M} be the compatible map such that $M = \widetilde{M} \circ \pi$. Since the map π is open and the map \widetilde{M} is a homeomorphism, the subset $M(\overset{\circ}{\Delta}_m)$ of Δ_X is open, so that $M(\overset{\circ}{\Delta}_m) \subset \overset{\circ}{\Delta}_X$.

On the other hand, the compact convex set Δ_X admits its extremal points among $\{X_1, \dots, X_m\}$. We first claim that any extremal point, say X_1 , is a limit point of $M(\overset{\circ}{\Delta}_m)$. In fact, since $X_1 - X_j$ ($j = 2, \dots, m$) are in a half-space, there is a vector $h \in \mathbb{R}^d$ such that $\langle h, X_1 - X_j \rangle > 0$ for all $j = 2, \dots, m$. Then the points

$$Y_n = \frac{\nabla Z(nh)}{Z(nh)} \in M(\overset{\circ}{\Delta}_m)$$

tend to X_1 (the argument holds even if some of X_j ($j \geq 2$) are equal to X_1 , such a case was not excluded). To finish the proof, it suffices to observe that any $\beta \in \overset{\circ}{\Delta}_X$ is a convex combination with strict positive coefficients of a set of points in $\overset{\circ}{\Delta}_X$, each of which is sufficiently close to an extremal point of Δ_X . It follows that $\beta \in M(\overset{\circ}{\Delta}_m)$. \square

The constraints (5.1) define a compact set on which the entropy function which is continuous attains its maximum. We will show that the entropy function attains its maximum at an interior point and the maximal point is unique if $\beta \in \overset{\circ}{\Delta}_X$.

Lemma 5.3. Assume $\beta \in \overset{\circ}{\Delta}_X$. Under the constraints (5.1), the entropy attains its maximum at a point $p^* \in \overset{\circ}{\Delta}_m$. Such maximal points are unique.

Proof. The uniqueness of maximal points is just because of the strict concavity of the entropy function.

Let p^* be the maximal point. Suppose that p^* is not strictly positive. Without loss of generality, we assume that $p_j^* > 0$ for $j = 1, \dots, k$, but $p_j^* = 0$ for $j = k+1, \dots, m$. Since $\beta \in \overset{\circ}{\Delta}_X$, by Lemma 5.2, there exists a probability vector $q \in \overset{\circ}{\Delta}_m$ such that $\beta = Mq$. Denote $r = q - p^*$. Then we have $Mr = 0$. Notice that $\sum_{i=1}^m r_i = 0$ and $r_j > 0$ for $j = k+1, \dots, m$. Consider the perturbation of p^* defined by

$$p_t = p^* + tr.$$

For small $t > 0$, p_t is a probability satisfying the constraint $Mp_t = \beta$. Then consider of function $f(t) = h(p_t)$, that is

$$f(t) = - \sum_{j=1}^m (p_j^* + tr_j) \log(p_j^* + tr_j).$$

Its derivative is equal to

$$f'(t) = - \sum_{j=1}^m r_j (\log(p_j^* + tr_j) + 1).$$

Let $\epsilon = \min_{1 \leq j \leq k} p_j^*$. Then for t small enough, we have

$$-r_j(\log(p_j^* + tr_j) + 1) \geq |r_j|(\log \epsilon/2 + 1), \quad \text{for } j = 1, \dots, k;$$

but as $t \rightarrow 0^+$,

$$-r_j(\log(p_j^* + tr_j) + 1) = -r_j \log(tr_j) - r_j \rightarrow \infty, \quad \text{for } j = k+1, \dots, m.$$

So we have $f'(t) > 0$ for small $t > 0$ and hence $f(t)$ is increasing near 0. This contradicts the maximality of $h(p^*)$. \square

Lemma 5.4. *There exists a unique point $t_\beta \in \mathbb{R}^d$ such that*

$$(5.4) \quad p_j^* = \frac{e^{\langle t_\beta, X_j \rangle}}{Z(t_\beta)}, \quad 1 \leq j \leq m.$$

This point t_β is the unique solution of the equation $\nabla Z(t)/Z(t) = \beta$. The maximal entropy $h(p^)$ is equal to $\log Z(t_\beta) - \langle t_\beta, \beta \rangle$.*

Proof. Consider the function

$$F(p, \lambda, t) = h(p) + \lambda \left(\sum_{j=1}^m p_j - 1 \right) + \left\langle t, \sum_{j=1}^m p_j X_j - \beta \right\rangle$$

where $p \in (\mathbb{R}^+)^m$, $\lambda \in \mathbb{R}$ and $t \in \mathbb{R}^d$. Both λ and t are Lagrange multipliers. The maximal point p^* whose existence is proved above must be the critical point of F . But

$$\frac{\partial F}{\partial p_j} = -\log p_j - 1 + \lambda + \langle t, X_j \rangle.$$

We deduce that the maximal point p^* is of the form

$$(5.5) \quad p_j^* = \frac{e^{\langle t, X_j \rangle}}{Z(t)}$$

for some t verifying $\nabla Z(t)/Z(t) = \beta$. By the way, we have proved that the equation $\nabla Z(t)/Z(t) = \beta$ admits a solution. We claim that there is a unique t verifying (5.5). Suppose $t' \neq t$ is another suitable point. Then

$$\frac{e^{\langle t, X_j \rangle}}{Z(t)} = \frac{e^{\langle t', X_j \rangle}}{Z(t')}, \quad \text{i.e.} \quad e^{\langle t-t', X_j \rangle} = \frac{Z(t)}{Z(t')}.$$

Then $e^{\langle t-t', X_i - X_j \rangle} = 1$, i.e. $\langle t - t', X_i - X_j \rangle = 0$ for all i, j . This contradicts that X_j 's are not coplanar. Clear $h(p^*) = \log Z(t_\beta) - \langle t_\beta, \beta \rangle$ where t_β is the unique point satisfying (5.5).

Now we prove that the equation $\nabla Z(t)/Z(t) = \beta$ admits a unique solution. Suppose that t' is another solution. We can check that the probability p' defined by $p'_j = e^{\langle t', X_j \rangle}/Z(t')$ is a maximal point. So, $p' = p^*$ and then $t' = t$. \square

Consider t_β as a function of $\beta \in \overset{\circ}{C}_X$. It is the inverse function of $t \mapsto A(t)$ where

$$A(t) = \frac{\nabla Z(t)}{Z(t)}.$$

Lemma 5.5. *The differential $dA(t)$ is non-singular at any point $t \in \mathbb{R}^d$. Hence $\beta \mapsto t_\beta$ is infinitely differentiable.*

Proof. Let $p(t)$ be the probability vector defined by $\nabla Z(t)/Z(t)$. Define the $m \times m$ matrix

$$G(t) = \text{diag}(p(t)) - p(t) \cdot p(t)^T,$$

where $\text{diag}(p(t))$ denotes the diagonal matrix with the elements of $p(t)$ as diagonal elements and $p(t)^T$ denotes the transpose of the column vector $p(t)$. A direct calculation shows that

$$dA(t) = MG(t)M^T.$$

Observe that $G(t)$ is symmetric and it defines the quadratic form

$$yG(t)y^T = \sum_{j=1}^m p_j y_j^2 - \left(\sum_{j=1}^m p_j y_j \right)^2.$$

If we introduce the inner product $(x, y) = \sum_{j=1}^m p_j x_j y_j$, by the Cauchy inequality we see that $G(t)$ is positive and $yG(t)y^T = 0$ iff y is parallel to $(1, 1, \dots, 1)$.

Suppose that $dA(t)$ is singular. Then $xMG(t)M^T x^T = 0$ for some $x \in \mathbb{R}^d$ with $x \neq 0$, i.e. $yG(t)y^T = 0$ for $y = xM$. By the properties of $G(t)$ proved above, $xM = c(1, 1, \dots, 1)$ for some $c \neq 0$, which means $\langle x, X_j \rangle = c$ for all j , i.e. X_1, \dots, X_m are coplanar. This is a contradiction. The infinite differentiability is a consequence of the implicit function theorem. \square

Finally, we consider the case that X_1, \dots, X_m are coplanar. Let H_0 be the subspace spanned by $X_i - X_j$ ($i, j = 1, 2, \dots, m$). Then $s := \dim H_0 < d$. We can apply the theorem if we replace \mathbb{R}^d by H_0 and t by vectors in H_0 . Then there is a unique t_β in H_0 associated to $\beta \in \overset{\circ}{C}_X$. We can also consider $t \in \mathbb{R}^d$. Then consider the orthogonal decomposition $\mathbb{R}^d = H_0 \oplus H_0^\perp$. For each $\beta \in \overset{\circ}{C}_X$, the solution of the equation $\nabla Z(t)/Z(t) = \beta$ is the set $t_\beta + H_0^\perp$ where $t_\beta \in H_0$.

6. Formula of $\gamma(\theta)$ in the coplanar case

In this section, we prove an formula for the growth function γ when X_1, \dots, X_m are coplanar. Let η be a non zero vector in \mathbb{R}^s , considered as the normal direction of a hyperplane. Recall that X_1, \dots, X_m are η -coplanar if

$$(6.1) \quad \forall j \in \{1, \dots, m\}, \quad \langle X_j, \eta \rangle = 1.$$

Denote by $H_\eta = \{X \in \mathbb{R}^s : \langle X, \eta \rangle = 1\}$ the hyperplane containing X_1, \dots, X_m . By the discussion of the previous section, we have

Lemma 6.1. *If β is an interior point in $H_\eta \cap \mathbf{C}_X$, then the solution t of the equation (5.3) exists and is unique up to a difference of $c\eta$ with $c \in \mathbb{R}$. Moreover, the entropy function $h(p) = -\sum_{j=1}^m p_j \log p_j$ with the constraint*

$$(6.2) \quad p_1 X_1 + \dots + p_m X_m = \beta.$$

attains it maximum at

$$(6.3) \quad p_j = \frac{e^{\langle t, X_j \rangle}}{Z(t)}, \quad 1 \leq j \leq m.$$

The function $Z(t)$ is conventionally called *partition function* and the probability given by (6.3) is called *Gibbs distribution*.

The vector t depends on β . In the following, we will consider $\beta = \frac{\theta}{\langle \theta, \eta \rangle}$, so t will depends on θ .

Proof of Theorem 1.3. For a fixed unit vector θ in the cone \mathbf{C}_X , put $\beta = \frac{\theta}{\langle \theta, \eta \rangle}$, which is the point on the hyperplane H_η of the direction θ .

Lower bound of $\gamma(\theta)$. Take any probability vector p satisfying the constraint (6.2). Let

$$(6.4) \quad n_j = \lfloor np_j \rfloor, \text{ for } j = 1, \dots, m-1 \text{ and } n_m = n - (n_1 + \dots + n_{m-1}).$$

It is clear that there exists a constant c independent of n (for example, $c = 3m \sum_{j=1}^m \|X_j\|$) such that

$$(6.5) \quad \left\| \sum_{j=1}^m n_j X_j - n\beta \right\| \leq c, \quad \sum_{j=1}^m |n_j - np_j| \leq c.$$

So, applying Theorem 3.3 with $C_0 = 2c$, we have

$$Q(n\|\beta\|)\mathbf{m}(n\beta) \geq \mathbf{m} \left(\sum_{j=1}^m n_j X_j \right) \geq \frac{n!}{n_1! \dots n_m!} \sim \frac{n!}{(np_1)! \dots (np_m)!},$$

where $Q(x)$ is the polynomial in Theorem 3.3, and $A \sim B$ means that A/B and B/A are bounded by a polynomial of n . Using Stirling's formula, we obtain that

$$\lim_{n \rightarrow \infty} \frac{\log \mathbf{m}(n\beta)}{n} \geq \log \frac{1}{p_1^{p_1} \dots p_m^{p_m}} = h(p).$$

Therefore

$$\gamma(\theta) = \lim_{k \rightarrow \infty} \frac{\log \mathbf{m}(k\theta)}{k} = \langle \theta, \eta \rangle \lim_{n \rightarrow \infty} \frac{\log \mathbf{m}(n\beta)}{n} \geq \langle \theta, \eta \rangle h(p).$$

Taking the supremum we get the following lower bound for $\gamma(\theta)$

$$\gamma(\theta) \geq \langle \theta, \eta \rangle \sup \{h(p) : p_1 X_1 + \dots + p_m X_m = \beta\}.$$

Upper bound of $\gamma(\theta)$. Let p be a probability vector such that $h(p)$ attains maximum under the restriction (6.2). Let (n_1, \dots, n_m) be the vector defined by (6.4). Let $x_n = n_1 X_1 + \dots + n_m X_m$. Then $|x_n - n\beta| \leq c$. Since p is the Gibbs distribution which is of exponential form (see (6.3)), for any (n'_1, \dots, n'_m) satisfying $n'_1 X_1 + \dots + n'_m X_m = x_n$, we have

$$p_1^{n'_1} \dots p_m^{n'_m} = \frac{\exp \langle t, n'_1 X_1 + \dots + n'_m X_m \rangle}{Z(t)^n} = \frac{\exp \langle t, x_n \rangle}{Z(t)^n}.$$

Now we consider a random walk: at any time, we forward the step X_j with the probability p_j . Then the above formula says that for any $\omega, \omega' \in \{1, 2, \dots, m\}^n$, as soon as $\kappa(\omega) = \kappa(\omega')$, both ω and ω' have the same probability. It follows that $Z(t)^{-n} \exp \langle t, x_n \rangle \mathbf{m}(x_n)$ is bounded by the probability that we arrive at x_n at time n , which is bounded by 1. Hence,

$$\mathbf{m}(x_n) \leq \frac{Z(t)^n}{\exp \langle t, x_n \rangle} = \frac{1}{p_1^{n_1} \dots p_m^{n_m}}.$$

As $n_j/n \rightarrow p_j$, we have

$$\lim_{n \rightarrow \infty} \frac{\log \mathbf{m}(x_n)}{n} \leq h(p).$$

Finally, since $\mathbf{m}(n\beta)/\mathbf{m}(x_n)$ is controlled by a polynomial of n , we obtain

$$\gamma(\theta) = \langle \theta, \eta \rangle \lim_{n \rightarrow \infty} \frac{\log \mathbf{m}(n\beta)}{n} \leq \langle \theta, \eta \rangle h(p).$$

This ends the proof of the theorem. \square

Theorem 6.2. *If X_1, \dots, X_m are η -coplanar, then for any unit vector θ in the interior of \mathbf{C}_X we have*

$$\gamma(\theta) = \langle \theta, \eta \rangle \log Z(t) - \langle t, \theta \rangle$$

where t is any solution stated in Lemma 6.1.

Proof. As we have seen in the above proof of Theorem 1.3, the supremum is attained at the Gibbs distribution $p_j = e^{\langle t, X_j \rangle} Z(t)^{-1}$. Taking the logarithm, we get

$$-\log p_j = \log Z(t) - \langle t, X_j \rangle.$$

Multiplying both sides by p_j and summing over j allow us to get

$$h(p) = \log Z(t) - \sum_{j=1}^m p_j \langle t, X_j \rangle = \log Z(t) - \langle t, \beta \rangle$$

where $\beta = \theta / \langle \theta, \eta \rangle$. Finally, we obtain the formula by multiplying $\langle \theta, \eta \rangle$. \square

The following proposition is an easy consequence of Theorem 1.3.

Proposition 6.3. *Assume that X_1, \dots, X_m are η -coplanar. Then*

$$\max \frac{\gamma(\theta)}{\langle \eta, \theta \rangle} = \log m \text{ at } \theta_0 = \frac{\sum_{j=1}^m X_j}{|\sum_{j=1}^m X_j|}.$$

The reason is that the entropy $h(p)$ attains its maximum $\log m$ at $p_1 = \dots = p_m = 1/m$. The corresponding direction on the hyperplane H_η is $\beta_0 = \frac{1}{m} \sum_{j=1}^m X_j$, the arithmetic average of X_1, X_2, \dots, X_m . The corresponding unit vector is θ_0 .

The growth of the semi-group has been defined as function of the unit vector θ . If we define the growth $\tilde{\gamma}(\beta)$ as function of the vector β located on the hyperplane H_η , we will get a simpler formula

$$\tilde{\gamma}(\beta) = \sup \{h(p) : p_1 X_1 + \dots + p_m X_m = \beta\} = \log Z(t) - \langle t, \beta \rangle.$$

This is the conditional variation principle for the multifractal analysis of the Birkhoff average

$$(6.6) \quad \lim_{n \rightarrow \infty} \frac{X_{\omega_1} + X_{\omega_2} + \dots + X_{\omega_n}}{n}.$$

See [6, 7, 8] for discussion in more general case. In general, it is difficult to determine exactly the possible limits of the Birkhoff average. Theorem 1.3 shows that for the special case of (6.6), the possible limit is the convex set $H_\eta \cap \mathbf{C}_X$.

7. Rigidity (I): Proof of Theorem 1.5

When the vectors X_1, \dots, X_m are η -coplanar, we have proved that the growth function is equal to

$$\gamma(\theta) = \langle \theta, \eta \rangle (\log Z(t) - \langle \beta, t \rangle)$$

where $\beta = \frac{\theta}{\langle \theta, \eta \rangle}$ and t is any solution of the equation $\nabla Z(t)/Z(t) = \beta$. The set of solutions of t is a line consisting of the points $t_\beta + c\eta$ ($c \in \mathbb{R}$) and we will choose the one such that the last coordinate of $t_\beta + c\eta$ is zero. It is really possible that the last coordinate is zero if $\eta_s \neq 0$. In fact, we can choose

$$c = -\frac{\langle t_\beta, e_s \rangle}{\langle \eta, e_s \rangle}$$

where $e_s = (0, \dots, 0, 1) \in \mathbb{R}^s$. The next lemma shows that it is possible to convert the general case to the case with $\eta_s =: \langle \eta, e_s \rangle \neq 0$.

Lemma 7.1. *Let $X = \{X_1, \dots, X_m\}$ be a set of integral vectors on \mathbb{Z}^s and let T be an invertible $s \times s$ matrix with integral entries.*

(i) *The function γ_{TX} is related to γ_X by the formula*

$$\gamma_{TX}(\theta) = \|T^{-1}\theta\| \gamma_X \left(\frac{T^{-1}\theta}{\|T^{-1}\theta\|} \right).$$

(ii) *If X is η -coplanar, then TX is $(T^*)^{-1}\eta$ -coplanar, where T^* is the transpose of T .*

Proof. (ii) is obvious. (i) is proved by computation. The key point is the observation $\mathbf{m}_{TX}(z) = \mathbf{m}_X(T^{-1}z)$. Then we have

$$\begin{aligned} \gamma_{TX}(\theta) &= \lim_{k \rightarrow \infty} \frac{\mathbf{m}_{TX}(k\theta)}{k} = \lim_{k \rightarrow \infty} \frac{\mathbf{m}_X(kT^{-1}\theta)}{k} \\ &= \lim_{k \rightarrow \infty} \frac{\mathbf{m}_X(kT^{-1}\theta)}{\|kT^{-1}\theta\|} \cdot \frac{\|kT^{-1}\theta\|}{k} = \|T^{-1}\theta\| \gamma_X \left(\frac{T^{-1}\theta}{\|T^{-1}\theta\|} \right). \end{aligned}$$

□

Theorem 1.5 and Theorem 1.6 compare two sets of vectors $X = \{X_1, \dots, X_m\}$ and $Y = \{Y_1, \dots, Y_{m'}\}$, which are respectively η -coplanar and η' -coplanar. Without loss of generality, we may assume that $\eta_s \neq 0$ and $\eta'_s \neq 0$. Otherwise we can consider the images of X and Y under a linear transformation T as stated in the last lemma. Actually, we may choose $a = (a_1, \dots, a_{s-1}, 1) \in \mathbb{Z}^s$ such that

$$\langle a, \eta \rangle \neq 0, \quad \langle a, \eta' \rangle \neq 0.$$

Such a 's do exist, because the condition $\langle z, \eta \rangle = 0$ or $\langle z, \eta' \rangle = 0$ defines a union of two hyperplanes and we can find points a outside these two hyperplanes. Define

$$T = \begin{pmatrix} 1 & & & -a_1 \\ & 1 & & -a_2 \\ & & \ddots & \vdots \\ & & & 1 & -a_{s-1} \\ & & & & 1 \end{pmatrix}.$$

Then we have the last coordinate of $T^{*-1}\eta$ is equal to $\langle a, \eta \rangle \neq 0$ and the last coordinate of $T^{*-1}\eta'$ is equal to $\langle a, \eta' \rangle \neq 0$.

From now on, we assume that X_1, \dots, X_m are η -coplanar vectors in \mathbb{Z}^s such that $\eta_s \neq 0$ and that there is a (unique) solution t of (5.3), i.e.

$$(7.1) \quad \sum_{j=1}^m (X_j - \beta) e^{\langle t, X_j \rangle} = 0$$

such that $t_s = 0$. We define

$$F(\beta) = \log Z(t) - \langle \beta, t \rangle,$$

which is a function on $\beta_1, \dots, \beta_{s-1}$ since $t_s = 0$. The variables $\beta_1, \dots, \beta_{s-1}$ are independent and (t_1, \dots, t_{s-1}) is a C^∞ map of $(\beta_1, \dots, \beta_{s-1})$. Notice that $F(\beta) = \langle \eta, \theta \rangle^{-1} \gamma(\theta)$.

Lemma 7.2. *Let X_1, \dots, X_m be η -coplanar vectors and $\eta_s \neq 0$. Then*

- (i) $\frac{\partial F}{\partial \beta_j} = -t_j$ for $j = 1, \dots, s-1$.
- (ii) $\sum_{j=1}^{s-1} \frac{\partial \gamma}{\partial \theta_j} \theta_j = \gamma(\theta) - \frac{\eta_s}{\theta_s} \log Z(t)$.

Proof. (i) Using the chain rule of derivation and the relation (7.1), we have

$$\frac{\partial F}{\partial \beta_j} = Z^{-1}(t) \sum_{\ell=1}^m e^{\langle t, X_\ell \rangle} \sum_{k=1}^{s-1} X_{\ell,k} \frac{\partial t_k}{\partial \beta_j} + \left(-t_j - \sum_{k=1}^{s-1} \beta_k \frac{\partial t_k}{\partial \beta_j} \right) = -t_j.$$

(ii) Let us denote $f(\theta) = \langle \eta, \theta \rangle$. Then $\beta = \theta/f(\theta)$ and $\gamma(\theta) = f(\theta)F(\beta)$. By the chain rule of differentiation, we have (\mathbf{e}_j denotes the j -th element of the canonical basis)

$$\begin{aligned} \frac{\partial \gamma}{\partial \theta_j} &= \frac{\partial f}{\partial \theta_j} F(\beta) + f \cdot \left(\frac{\partial F}{\partial \beta_1}, \dots, \frac{\partial F}{\partial \beta_{s-1}} \right) \times \left(-\frac{\partial f / \partial \theta_j}{f^2} \begin{pmatrix} \theta_1 \\ \vdots \\ \theta_{s-1} \end{pmatrix} + \frac{1}{f} \mathbf{e}_j \right) \\ &= \frac{\partial f}{\partial \theta_j} \left(F(\beta) + \frac{\langle t, \theta \rangle}{f} \right) - t_j \\ &= \frac{\partial f}{\partial \theta_j} \log Z(t) - t_j, \end{aligned}$$

where \times stands for the matrix product. Since $\theta_s^2 = 1 - \sum_{j=1}^{s-1} \theta_j^2$, we have $\frac{\partial f}{\partial \theta_j} = \eta_j - \frac{\eta_s}{\theta_s} \theta_j$, and hence

$$(7.2) \quad \frac{\partial \gamma}{\partial \theta_j} = \left(\eta_j - \frac{\eta_s}{\theta_s} \theta_j \right) \log Z(t) - t_j, \quad j = 1, \dots, s-1.$$

Therefore

$$\sum_{j=1}^{s-1} \frac{\partial \gamma(\theta)}{\partial \theta_j} \theta_j = \left(\langle \eta, \theta \rangle - \frac{\eta_s}{\theta_s} \right) \log Z(t) - \langle t, \theta \rangle = \gamma(\theta) - \frac{\eta_s}{\theta_s} \log Z(t).$$

□

Proof of Theorem 1.5. According to Lemma 7.1 and the discussion just before Lemma 7.1, we may assume without loss of generality that $\eta_s \neq 0$ and $\eta'_s \neq 0$. Otherwise, we consider TX and TY for some suitable integral invertible transformation T .

First, we claim that $m = m'$. By Proposition 6.3, the functions $\langle \eta, \theta \rangle^{-1} \gamma_X$ and $\langle \eta, \theta \rangle^{-1} \gamma_Y$ attain their respective maximum $\log m$ and $\log m'$. As γ_X and γ_Y are the same function, we get $\log m = \log m'$, so that $m = m'$.

Next, applying Lemma 7.2 (i) to X , we get

$$(7.3) \quad t_j = -\partial F / \partial \beta_j, \quad j = 1, \dots, s-1.$$

Similarly, we get

$$(7.4) \quad \tilde{t}_j = -\partial \tilde{F} / \partial \beta_j, \quad j = 1, \dots, s-1$$

where

$$\tilde{F}(\beta) = \log \tilde{Z}(\tilde{t}) - \langle \beta, \tilde{t} \rangle, \quad \tilde{Z}(\tilde{t}) = \sum_{j=1}^m e^{\langle \tilde{t}, Y_j \rangle}$$

and \tilde{t} is the solution of $\nabla \tilde{Z}(\tilde{t}) / \tilde{Z}(\tilde{t}) = \beta$ such that $\tilde{t}_s = 0$.

Since $\gamma_X(\theta) = \gamma_Y(\theta)$, $F(\beta) = \tilde{F}(\beta)$ so that $t = \tilde{t}$ by (7.3) and (7.4). Therefore $Z(t) = \tilde{Z}(t)$, i.e.,

$$\sum_{j=1}^m e^{\langle t, X_j \rangle} = \sum_{j=1}^m e^{\langle t, Y_j \rangle}.$$

In this equality, t is a function of $\hat{\beta} = (\beta_1, \dots, \beta_{s-1})$ and $\hat{\beta}$ varies in a open set of \mathbb{R}^{s-1} . The function $\hat{\beta} \mapsto t$ is actually a diffeomorphism. So, t varies in a open set U of \mathbb{R}^{s-1} .

Consider the polynomial

$$P(z_1, \dots, z_{s-1}) := \sum_{j=1}^m z^{\hat{X}_j} - \sum_{j=1}^m z^{\hat{Y}_j} = \sum_{j=1}^m \prod_{k=1}^{s-1} z_k^{X_{j,k}} - \sum_{j=1}^m \prod_{k=1}^{s-1} z_k^{Y_{j,k}}$$

where $z = (z_1, \dots, z_{s-1})$ and $\hat{X}_j = (X_{j,1}, \dots, X_{j,s-1})$. The above proved equality $Z(t) = \tilde{Z}(t)$ means that $P(z_1, \dots, z_{s-1}) = 0$ when $z_k = e^{t_k}$ for $k = 1, \dots, s-1$. The polynomials $\sum_{j=1}^m z^{\hat{X}_j}$ and $\sum_{j=1}^m z^{\hat{Y}_j}$ being equal in the open set $\{(e^{t_1}, \dots, e^{t_{s-1}}) : (t_1, \dots, t_{s-1}) \in U\}$, the exponents $\{\hat{X}_1, \dots, \hat{X}_m\}$ must be a permutation of the exponents $\{\hat{Y}_1, \dots, \hat{Y}_m\}$. Therefore $\{X_1, \dots, X_m\}$ is a permutation of $\{Y_1, \dots, Y_m\}$. \square

Remark 7.3. Here is an another argument for proving the equality $Z(t) = \tilde{Z}(t)$. Notice that F and \tilde{F} are Legendre transforms of the convex functions $\log N$ and $\log \tilde{N}$. Then $\log N$ and $\log \tilde{N}$ are the Legendre transforms of F and \tilde{F} . Since $F = \tilde{F}$, we get $\log N = \log \tilde{N}$ so that $N = \tilde{N}$.

8. Rigidity (II): Proof of Theorem 1.6

It is assumed that $\mathbf{C}_X = \mathbf{C}_Y$. We shall denote the common cone by \mathbf{C} .

If we do not have the information that η' is a multiple of η , it may happen that $t \neq \tilde{t}$ where t and \tilde{t} correspond to the same β (see the last section for notation). We will use another correspondence between β and the solutions t of $\nabla Z(t)/Z(t) = \beta$.

8.1. Standard solution. We call a solution t in Lemma 6.1 a *standard solution* if $Z(t) = 1$.

Lemma 8.1. *If t is a solution in Lemma 6.1, then the standard solution is*

$$t' = t - (\log Z(t)) \eta.$$

Proof. Let t be a solution in Lemma 6.1. Let $t' = t + d\eta$. Then $Z(t') = e^d Z(t)$ and $Z(t') = 1$ when $d = -\log Z(t)$. \square

Lemma 8.2. *Let X and Y are two collections of coplanar vectors with $\eta_s \neq 0$ and $\eta'_s \neq 0$. If $\gamma_X = \gamma_Y$, then for any θ belongs to the interior of \mathbf{C} , they have the same standard solution, i.e.,*

$$t' = (\tilde{t})'.$$

Proof. Let t be the solution in Lemma 6.1 with $t_s = 0$, then the s -th coordinate of the corresponding standard solution is $t'_s = -\eta_s \log Z(t)$. Similarly, we have $(\tilde{t})'_s = -\eta'_s \log \tilde{Z}(\tilde{t})$. Hence, by Lemma 7.2 (ii), we get

$$t'_s = -\eta_s \log Z(t) = -\eta'_s \log \tilde{Z}(\tilde{t}) = (\tilde{t})'_s.$$

For $j = 1, \dots, s-1$, using (7.2),

$$t'_j = t_j - \eta_j \log Z(t) = -\frac{\partial \gamma}{\partial \theta_j} - \frac{\theta_j}{\theta_s} \eta_s \log Z(t) = -\frac{\partial \gamma}{\partial \theta_j} + \frac{\theta_j}{\theta_s} t'_s.$$

So $t'_j = (\tilde{t})'_j$. □

Let $z = (z_1, \dots, z_s)$ and $n = (n_1, \dots, n_s)$. Denote $z^n = z_1^{n_1} \cdots z_s^{n_s}$, and define

$$P(z) = \sum_{j=1}^m z^{X_j}, \quad Q(z) = \sum_{j=1}^{m'} z^{Y_j}.$$

Lemma 8.3. *Under the assumptions of Lemma 8.2, the algebraic equations $P(z) = 1$ and $Q(z) = 1$ have infinitely many common solutions.*

Proof. Notice that $P(e^t) = Z(t)$ and $Q(e^t) = \tilde{Z}(t)$ where $e^t := (e^{t_1}, \dots, e^{t_s})$. For any θ belongs to the interior of \mathbf{C} , let t' be the corresponding standard solution. Then $e^{t'} = e^{(\tilde{t})'}$ is a common solution of $P(z) = 1$ and $Q(z) = 1$. □

8.2. H_η and $H_{\eta'}$ are parallel when $s = 2$. We will reduce Theorem 1.6 to Theorem 1.5. The key point is to show that H_η and $H_{\eta'}$ are parallel. Essentially we only need to prove the parallelism in the two-dimensional case and the general case will be reduced to this special case. In the following, we only need the above lemmas in the two-dimensional case.

First, we recall some basic definitions and facts on algebraic plane curve.

An *algebraic plane curve* is a curve consisting of the points of the plane whose coordinates x, y satisfy an equation $f(x, y) = 0$ for some $f \in \mathbb{R}[x, y]$. The curve is said to be *irreducible* if f is an irreducible polynomial. It is well-known the polynomial ring $\mathbb{R}[x, y]$ is a unique factorization domain, that is, any polynomial f has a unique factorization

$f = f_1 \dots f_n$ (up to constant multiples) as a product of irreducible factors f_j . Hence, every algebraic curve is a union of several irreducible algebraic curves. The following lemma is fundamental, see for example [15].

Lemma 8.4 ([15]). *Let $f \in \mathbb{R}[x, y]$ and $g \in \mathbb{R}[x, y]$ be two polynomials. Suppose that f is irreducible polynomial and is not a factor of g . Then the system of equations*

$$f(x, y) = g(x, y) = 0$$

has only a finite number of solutions.

Let $f(x, y)$ be a polynomial. A *highest term* of f is a term of f whose degree is equal to the degree of f . The homogenous polynomial consisting of all the highest terms of f will be denoted by H_f . It is called the *principal part* of f . For example, if $f(x, y) = ax^2 + bxy + cy^2 + dx + ey + f$, then $H_f(x, y) = ax^2 + bxy + cy^2$.

Theorem 8.5. *Suppose $X = \{X_1, \dots, X_m\} \subset \mathbb{Z}^2$ is η -coplanar and $Y = \{Y_1, \dots, Y_{m'}\} \subset \mathbb{Z}^2$ is η' -coplanar, and that X and Y define the same directional growth function. Then $\eta = c\eta'$ for some $c > 0$. In other words, the line containing X and the line containing Y are parallel.*

Proof. By applying a suitable linear transformation, we may assume that $\mathbf{C} = (\mathbb{R}^+)^2$ and $X_1, \dots, X_m, Y_1, \dots, Y_{m'} \in \mathbb{N}^2$ (see Lemma 7.1.) We can further assume that $\eta = (1/n, 1/n)$ for some integer $n \geq 1$. Indeed, let (x_1, y_1) and (x_2, y_2) be two vectors in X locating on two boundary rays of $\mathbf{C} = \mathbf{C}_X = \mathbf{C}_Y$, respectively. Let T be the linear transformation which maps (x_1, y_1) and (x_2, y_2) to $(1, 0)$ and $(0, 1)$, respectively. Clearly T is invertible, and the entries of T belong to \mathbb{Q} . It follows that $T(x, y) \in \mathbb{Q}^2$ for all $(x, y) \in X \cup Y$. Hence, there exists a positive integer n such that nT is an integral matrix, and $nT(x, y)$ are integral vectors for all $(x, y) \in X \cup Y$. It is seen that nT is the desired transformation.

Our aim is then to show that $\eta' = (c, c)$ for some $c > 0$. Consider the polynomials

$$P(x, y) = \sum_{j=1}^m x^{X_{j,1}} y^{X_{j,2}}, \quad Q(x, y) = \sum_{j=1}^{m'} x^{Y_{j,1}} y^{Y_{j,2}}.$$

By Lemma 8.3, $P(x, y) - 1 = 0$ and $Q(x, y) - 1 = 0$ have infinitely common roots. Hence, by Lemma 8.4, $P(x, y) - 1$ and $Q(x, y) - 1$ have a common non-trivial factor. Let us denote their greatest common factor by $S(x, y)$.

We claim that the principal part $H_S(x, y)$ of $S(x, y)$ contains at least two terms. Let $P(x, y) - 1 = S(x, y)T(x, y)$. Since $P(x, y)$ is homogenous,

$$H_S(x, y) \cdot H_T(x, y) = H_P(x, y) = P(x, y).$$

Suppose that $H_S(x, y)$ is a monomial, say, $H_S(x, y) = x^p y^q$. Then it must divide each term of $P(x, y)$, including x^n and y^n (Notice that x^n and y^n are two terms in $P(x, y)$ with the coefficients different from 0). It is impossible and our claim is thus proved.

Let $Q(x, y) - 1 = S(x, y)R(x, y)$. Then

$$H_S(x, y) \cdot H_R(x, y) = H_Q(x, y).$$

So $H_Q(x, y)$ has at least two terms. Therefore, $Q(x, y)$ has two terms with the same degree. That is to say, there exist two different integers i and j such that

$$(Y_{i,1}, Y_{i,2}) \neq (Y_{j,1}, Y_{j,2}), \quad Y_{i,1} + Y_{i,2} = Y_{j,1} + Y_{j,2}.$$

Recall that

$$\eta'_1 Y_{i,1} + \eta'_2 Y_{i,2} = 1, \quad \eta'_1 Y_{j,1} + \eta'_2 Y_{j,2} = 1.$$

Then solving η'_1 and η'_2 as unknown leads to

$$\eta'_1 = \frac{Y_{j,2} - Y_{i,2}}{D} = \frac{Y_{i,1} - Y_{j,1}}{D} = \eta'_2$$

where $D = Y_{i,1}Y_{j,2} - Y_{i,2}Y_{j,1} \neq 0$. Thus we have proved $\eta' = c\eta$ for some c . \square

8.3. Proof of Theorem 1.6. The proof of Theorem 1.6 is decomposed into several lemmas.

Lemma 8.6. *Let $X = \{X_1, \dots, X_m\}$ and $X^{(p)}$ denotes the p -th iteration of X . Then*

- (i) *X and $X^{(p)}$ defines the same directional growth function.*
- (ii) *If X is η -coplanar, then $X^{(p)}$ is η/p -coplanar.*

Proof. (ii) is obvious. In the following, we prove (i). Let us denote

$$X^{(p)} = \{W_1, \dots, W_{m^p}\}$$

which is the set of all $\sum_{j=1}^p X_{\omega_j}$ with $\omega_1 \dots \omega_p \in \{1, \dots, m\}^p$. Notice that many vectors in $X^{(p)}$ are repeated. For example, $X_1 + X_2 + \dots + X_m$ and $X_m + \dots + X_2 + X_1$ are the same. Let

$$\mathcal{J} = X_1\mathbb{N} + \dots + X_m\mathbb{N}, \quad \mathcal{J}' = W_1\mathbb{N} + \dots + W_{m^p}\mathbb{N}.$$

Then $\mathcal{J}' \subset \mathcal{J}$ and \mathcal{J}' is relatively dense in \mathcal{J} . Moreover, take any $z \in \mathcal{J}'$ and let $\omega_1 \dots \omega_n \in \{1, \dots, m\}^n$ be a path relative to the walk guided by X such that

$$z = \sum_{j=1}^n X_{\omega_j}.$$

Then n must be a multiple of p . Write

$$z = \sum_{k=1}^{n/p} \sum_{j=1}^p X_{\omega_{j+(k-1)p}}.$$

Hence $(\omega_1 \dots \omega_p)(\omega_{p+1} \dots \omega_{2p}) \dots (\omega_{n-p+1} \dots \omega_n)$ is a path relative to the walk guided by $X^{(p)}$. Therefore $\mathbf{m}_X(z) = \mathbf{m}_{X^{(p)}}(z)$ for all $z \in \mathcal{J}'$. It follows that they define the same direction growth function. \square

Let us recall some notions on convex set (see [14]). A *face* of a convex set C is a convex subset C' of C such that every closed line segment in C with a relative interior point in C' has both end points in C' . A vertex (i.e. an extremal point) of a convex set C is regarded as a 0-dimensional face. A face of dimension 1 is conventionally called an *edge*.

If $C = \mathbf{C}_X$, then the only 0-dimensional face is the origin, a 1-dimensional face is also called an *extreme ray*.

A set is called a *polytope* if it is the convex hull of finitely many points.

Lemma 8.7. *Under the condition of Theorem 1.6, we have $\eta = c\eta'$ for some $c > 0$.*

Proof. Let D be a two-dimensional face of \mathbf{C} . Let $X_D = X \cap D$ be the collection of X_j which locates in D . Similarly, we define Y_D . Clearly X_D and Y_D are coplanar collections.

Let us define a Frobenius problem with defining data X_D . Let \mathcal{J}' be the semi-group generated by X_D . For $z \in \mathcal{J}'$, as before, we define $\mathbf{m}_{X_D}(z)$ to be the number of paths terminated at z . Since D is a face, $X_{i_1} + \dots + X_{i_k}$ is in D only if all the vectors X_{i_j} belongs to X_D , so $\mathbf{m}_{X_D}(z) = \mathbf{m}_X(z)$ for all $z \in \mathcal{J}'$. For $x \in \mathbf{C}_{X_D}$, we define $\mathbf{m}_{X_D}(x)$ to be the multiplicity of the element in \mathcal{J}' nearest to x . By Theorem 3.3, the ratio of $\mathbf{m}_X(x)$ and $\mathbf{m}_{X_D}(x)$ is controlled by a polynomial on $\|x\|$. Now, we define the directional growth function

$$\gamma_{X_D}(\theta) = \lim_{k \rightarrow \infty} \frac{\log \mathbf{m}_{X_D}(k\theta)}{k}.$$

Then $\gamma_{X_D}(\theta) = \gamma_X(\theta)$. Similarly, we define a Frobenius problem with defining data Y_D . It turns out that

$$\gamma_{X_D}(\theta) = \gamma_X(\theta) = \gamma_Y(\theta) = \gamma_{Y_D}(\theta).$$

Therefore, by Theorem 8.5, the line containing X_D is parallel to the line containing Y_D , so there is a constant c_D such that $y = c_D x$ as soon as $x \in X_D$ and $y \in Y_D$ are located on a same line.

Clearly $K_\eta = \mathbf{C}_X \cap H_\eta$ is the polytope generated by X . Let V_η be the vertex set of K_η . Clearly $V_\eta \subset X$. Similarly we define $K_{\eta'}$ and $V_{\eta'}$.

For any $x \in V_\eta$, there is a point $y \in V_{\eta'}$ such that x and y are located on a same extremal ray of \mathbf{C} . Let $c_x > 0$ be the real number such that $y = c_x x$.

If x and x' are the two end points of an edge of K_η , this edge determines a two dimensional face D of \mathbf{C} . Then $c_x = c_{x'} = c_D$ by the above discussion. Take two arbitrary points $x, x'' \in V_\eta$, there always exists a path (consisting of edges of K_η) from x to x'' . We deduce that $c_x = c_{x''}$.

Let us denote this common constant by c . Then for any $y \in V_{\eta'}$,

$$\langle y, c^{-1}\eta \rangle = \langle cx, c^{-1}\eta \rangle = \langle x, \eta \rangle = 1.$$

Since the points in $V_{\eta'}$ span the space \mathbb{R}^d , we have $c^{-1}\eta = \eta'$, i.e. $\eta = c\eta'$. \square

Lemma 8.8. *The constant c in the last lemma is a rational number.*

Proof. Since the points in X are integral, solving $\langle X_j, \eta \rangle = 1$ by Cramer rule, we get the solution η , whose entries are rational numbers. The entries of η' are also rational numbers. It follows that c is a rational number. \square

Proof of Theorem 1.6. Let us write $c = q/p$. Consider $X^{(q)}$, the q -th iteration of X , and $Y^{(p)}$, the p -th iteration of Y . Both of them are (η/q) -coplanar and define the same directional growth function by Lemma 8.6. Therefore, by Theorem 1.5, $X^{(q)}$ is a permutation of $Y^{(p)}$. \square

Acknowledgement. The authors would like to thank Jia-yan Yao and Alain Rivi re for helpful discussions.

REFERENCES

- [1] J. Ramirez Alfonsin, *The Diophantine Frobenius problem*, Oxford Univ. Press, 2005.
- [2] R. D. Carmichael, *On sequences of integers defined by recurrence relations*, Quart. J. Math. **41** (1920), 343–372.
- [3] D. Cooper and T. Pignataro, *On the shape of Cantor sets*, J. Differential Geom., **28** (1988), 203–221.
- [4] G. David and S. Semmes, *Fractured fractals and broken dreams : self-similar geometry through metric and measure*, Oxford Univ. Press, 1997.
- [5] K. J. Falconer and D. T. Marsh, *On the Lipschitz equivalence of Cantor sets*, Mathematika, **39** (1992), 223–233.
- [6] A. H. Fan and D. J. Feng, *On the distribution of long-term time averages on symbolic space*, J. Statist. Phys., **99** (2000), 813–856.
- [7] A. H. Fan, D. J. Feng and J. Wu, *Recurrence, dimension and entropy*, J. London Math. Soc., **64** (2001), 229–244.

- [8] A. H. Fan, L. M. Liao and J. Peyrière, *Generic points in systems of specification and Banach valued Birkhoff ergodic average*, Discrete & cont. dyn. sys., **21** (2008), 1103–1128.
- [9] E. T. Jaynes, *Information Theory and Statistical Mechanics*, Physical Review. Series II 106 (4) (1957), 620–630.
- [10] J. J. Luo and K. S. Lau, *Lipschitz equivalence of self-similar sets and hyperbolic boundaries*, Adv. Math. **235** (2013), 555–579.
- [11] H. Rao, H. J. Ruan, and Y. Wang, *Lipschitz equivalence of Cantor sets and algebraic properties of contraction ratios*, Trans. Amer. Math. Soc., **364** (2012), 1109–1126.
- [12] H. Rao, H. J. Ruan and Y. Wang, *Lipschitz equivalence of self-similar sets: algebraic and geometric properities*, Contemp. Math., **600** (2013).
- [13] H. Rao and Y. Zhang, *Higer dimensional Frobenius problem and Lipschitz equivalence of Cantor sets*, Preprint 2014.
- [14] R. T. Rockafellar, *Convex Analysis*, Princeton University Press, Princeton, 1970.
- [15] I. Shafarevich, *Basic Algebraic Geometry*, Second edition, Springer-Verlag, Berlin, 1994.
- [16] J. J. Sylvester, *Mathematical questions with their solutions*, Education Times **41-21** (1884).
- [17] L.F. Xi and Y. Xiong, *Lipschitz Equivalence Class, Ideal Class and the Gauss Class Number Problem*. Preprint 2013 (arXiv:1304.0103 [math.MG]).

DEPARTMENT OF MATHEMATICS AND STOCHASTIC, HUA ZHONG NORMAL UNIVERSITY, WUHAN 430072,
CHINA & UMR 7352, CNRS, UNIVERSITÉ DE PICARDIE, 33 RUE SAINT LEU, 80039 AMIENS, FRANCE
E-mail address: `ai-hua.fan@u-picardie.fr`

DEPARTMENT OF MATHEMATICS AND STOCHASTIC, HUA ZHONG NORMAL UNIVERSITY, WUHAN 430072,
CHINA
E-mail address: `hrao@mail.ccnu.edu.cn`

DEPARTMENT OF MATHEMATICS AND STOCHASTIC, HUA ZHONG NORMAL UNIVERSITY, WUHAN 430072,
CHINA
E-mail address: `hrao@mail.ccnu.edu.cn`